Supreme Court, U.S.
FILED
AUG 5 1991
OFFICE OF THE CLERK

(2)

No. 90-1876

In the Supreme Court of the United States

OCTOBER TERM, 1991

ROBERT TAPPAN MORRIS, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

KENNETH W. STARR
Solicitor General

ROBERT S. MUELLER, III
Assistant Attorney General

MARK D. RASCH
ELLEN R. MELTZER
Attorneys
Department of Justice
Washington, D.C. 20530
(202) 514-2217

QUESTION PRESENTED

Whether, under 18 U.S.C. 1030(a)(5)(A), the government must prove both that petitioner intended to access computers without authorization and that he intended to prevent the authorized use of the computers and to cause monetary loss to their owners.

TABLE OF CONTENTS

	Page
Opinion below	1
Jurisdiction	1
Statement	1
Argument	5
Conclusion	9

TABLE OF AUTHORITIES

Cases:

INS v. *Cardoza-Fonseca*, 480 U.S. 421 (1987)	8
International Primate Protection League v. *Administrators of Tulane Educ. Fund*, 111 S. Ct. 1700 (1991)	5-6
Liparota v. *United States*, 471 U.S. 419 (1985)	6, 7
Morissette v. *United States*, 342 U.S. 246 (1952)	7
United States v. *Johnson & Towers, Inc.*, 741 F.2d 662 (3d Cir. 1984), cert. denied, 469 U.S. 1208 (1985)	7
United States v. *Nofziger*, 878 F.2d 442 (D.C. Cir.), cert. denied, 110 S. Ct. 564 (1989)	6, 7
United States v. *Ron Pair Enterprises*, 489 U.S. 235 (1989)	5
United States v. *United States Gypsum Co.*, 438 U.S. 422 (1978)	7
United States v. *Yermian*, 468 U.S. 63 (1984)	6

Statutes:

Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213	7
18 U.S.C. 1030	5
18 U.S.C. 1030(a)(3)	6
18 U.S.C. 1030(a)(3) (Supp. II 1984)	7
18 U.S.C. 1030(a)(5)	5
18 U.S.C. 1030(a)(5)(A)	2, 3, 4, 5, 7
18 U.S.C. 1030(e)(2)	2

Miscellaneous: Page

H.R. 3381, 99th Cong., 1st Sess. (1985) 8
H.R. Rep. No. 612, 99th Cong., 2d Sess. (1986) 8
S. 440, 99th Cong., 2d Sess. (1985) 8
S. 610, 99th Cong., 1st Sess. (1985) 8
S. 1678, 99th Cong., 1st Sess. (1985) 8
S. Rep. No. 432, 99th Cong., 2d Sess. (1986) 7-8, 8

In the Supreme Court of the United States

OCTOBER TERM, 1991

No. 90-1876

ROBERT TAPPAN MORRIS, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINION BELOW

The opinion of the court of appeals (Pet. App. 1a-19a) is reported at 928 F.2d 504.

JURISDICTION

The judgment of the court of appeals was entered on March 7, 1991. The petition for a writ of certiorari was filed on June 5, 1991. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

After a jury trial in the United States District Court for the Northern District of New York, petitioner was convicted on one count of intentionally accessing without authorization numerous "Federal

interest computers," thereby causing losses of more than $1,000 to the computers' owners, in violation of 18 U.S.C. 1030(a)(5)(A). The district court sentenced petitioner to three years' probation and a $10,000 fine. The court of appeals affirmed. Pet. App. 1a-19a.

1. In 1988, petitioner was a computer science graduate student at Cornell University. During the fall of that year, he designed a computer program called a "worm," which had the capacity to replicate itself as it infiltrated computers that were linked by a computer network. In November of 1988, petitioner intentionally released the worm into the INTERNET network, a nationwide computer network that was protected by federal law, see 18 U.S.C. 1030(e)(2), and that petitioner had no authorization to access in the way he did. Pet. App. 3a, 4a, 14a-19a. Although the worm was not intended to harm the computers it infected, its rapid multiplication ultimately caused numerous computers that used the network to "crash" (*i.e.*, shut down automatically) or otherwise cease to function, thereby preventing the proper, authorized use of thousands of government, military, educational, and commercial computers for up to several days, resulting in substantial monetary losses. *Id.* at 6a.

Petitioner programmed the worm to spread as widely as possible over the INTERNET network, but to be difficult to detect, eradicate, and trace back to him. Pet. App. 4a; Gov't C.A. Br. 7, 9-11. In order to gain access to as many computers as possible, petitioner designed the worm to use various unauthorized methods of entry, such as "cracking," or guessing the passwords of legitimate users. Pet. App. 5a. To make the worm inconspicuous, petitioner programmed

it not to reproduce more than a few times on any computer. *Id.* at 4a.

The worm program behaved precisely as petitioner intended it to, with one exception: an error in the program caused the worm to reproduce far more rapidly than anticipated. That flaw resulted in the replication of multiple worms on many INTERNET computers, rather than the small number of copies originally contemplated. So many copies were reproduced onto the affected computers that the worm program itself began to take up all of the computers' processing time, causing those systems to crash. Pet. App. 5a-6a.

2. Both in the district court and in the court of appeals, petitioner argued that 18 U.S.C. 1030(a)(5)(A) required the government to show not only that petitioner intentionally accessed computers without authorization, which the government proved, but also that petitioner intended to prevent authorized users from using the computers and that he intended to cause monetary losses to the operators of those computers, which the government did not prove. Pet. App. 7a, 48a.

The district court ruled that the statute was "clear and unambiguous," that "the requirement of intent is only applicable to the conduct of the 'accessing' and is unrelated to the resulting damage." Pet. App. 48a. The district court also concluded that the legislative history supported its construction of the statute. *Id.* at 48a-49a. The court accordingly instructed the jury that the government did not have to prove petitioner's specific intent to cause damage, and it denied petitioner's motions to dismiss and for a judgment of acquittal. Pet. 7.

The court of appeals affirmed. Although the court did not find the statutory language "so clear as to

preclude review of the legislative history," Pet. App. 8a, it nonetheless found from the legislative materials that Congress intended to require proof of intent only with respect to the unauthorized accessing of computers. *Id.* at 13a. Specifically, the court of appeals analyzed the predecessor statute to Section 1030(a)(5)(A) and concluded that Congress's modification of the *mens rea* requirement from "knowingly" under the former law to "intentionally" under the current provision was meant to protect those who accidentally gain access to computer files. That change, the court determined, indicated that the harm Congress wanted to punish was the intentional unauthorized accessing of computer equipment, and that intent to cause damage by means of that access was not required. Pet. App. 8a-10a. Moreover, the court noted, the original statute contained two expressions of the *mens rea* requirement, once before the access provision and once before the damage provision; the deletion of the *men rea* requirement before the damages section of the new statute indicated that Congress meant the intent requirement to apply only to access and not to damage. *Id.* at 10a-13a. The court of appeals concluded that "the wording, structure, and purpose of the subsection, examined in comparison with its departure from the format of its predecessor provision persuade us that the 'intentionally' standard applies only to the 'accesses' phrase of [the statute], and not to its 'damages' phrase." *Id.* at 13a.[1]

---

[1] The court of appeals also rejected petitioner's argument that the statute is ambiguous, and that the government had failed to prove that petitioner had gained access to the affected computers "without authorization." Pet. App. 14a-19a. Those issues are not presented for review. Pet. 7 n.4.

ARGUMENT

Petitioner renews his contention (Pet. 8-12) that 18 U.S.C. 1030(a)(5) requires proof of intent not only to access computers without authorization, but also to prevent use of the computers by authorized users and to cause loss to others. Because this is the first case to arise under 18 U.S.C. 1030, and there is accordingly no disagreement between the courts of appeals on the issue presented here, review by this Court is unwarranted. In any event, the court of appeals' decision is correct.

Section 1030(a)(5)(A) makes it illegal to "intentionally access[] a * * * computer without authorization, and by means of one or more instances of such conduct * * * prevent[] authorized use of any such computer * * * and thereby cause[] loss to one or more others of a value aggregating $1,000 or more during any one year period." The natural reading of that provision suggests that the modifier "intentionally" applies only to the "access" clause, and not to the "prevention of use" or "loss" clauses.

The punctuation and structure of the statute support that construction. The access provision, which is modified by the term "intentionally," appears in a separate phrase from the damage provisions. It is set off from the damage provisions by a comma, the conjunction "and," and the clause "by means of one or more instances of such conduct." The comma, conjunction, and "by means of" clause operate to differentiate the unauthorized access from the damages caused by that access. As a result, the access phrase "stands independent of the language that follows" it. *United States* v. *Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989); see *International Primate Protection League* v. *Administrators of Tulane Educ. Fund*,

111 S. Ct. 1700, 1705-1706 (1991); *United States* v. *Yermian*, 468 U.S. 63, 68-69 (1984). The terms "thereby" and "by means of" further separate the access provision from the damage provisions and establish the requirement that there be a connection between the intentional access and the damage that results from that access. The structure of the statute makes it apparent that the behavior Congress sought to criminalize was the intentional unauthorized accessing of computers; the remainder of the statute is meant to limit the criminal sanction to those instances where the illegal access causes substantial damage.[2] That reading of the statute makes sense, because deterring unauthorized entry would itself protect against the type of harm caused by such entry.

The cases on which petitioner relies are not to the contrary. The statute at issue in *Liparota* v. *United States*, 471 U.S. 419 (1985), did not contain discrete phrases, each set off by a buffer of commas and conjunctions. Moreover, the interpretation of the statute that *Liparota* rejected would not have required the violator to have had any level of intent with respect to any element of the crime—in other words, the rejected interpretation would have created a strict liability crime that covered both culpable and non-culpable behavior. See *id.* at 425-432. Likewise, in *United States* v. *Nofziger*, 878 F.2d 442 (D.C. Cir.), cert. denied, 110 S. Ct. 564 (1989), the structural and grammatical separation between statutory phrases was far less sharp than in this case, and the court was concerned that the government's interpretation of the statute could "criminalize a broad range

---

[2] In cases in which no damage results from the unauthorized access, the statute provides for a misdemeanor penalty. See 18 U.S.C. 1030(a)(3).

of apparently innocent conduct." *Id.* at 453, quoting *Liparota*, 471 U.S. at 426.[3] In this case, unlike in *Liparota* and *Nofziger*, the government's interpretation of the statute would not create a strict liability crime; rather, a violator must intend to break into a computer, and only then would he be liable for the damage caused by the illicit entry. It could come as no surprise to petitioner that once he had intentionally invaded a computer system, he could be held accountable for the damage he caused there.

The legislative history of the Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, ——, 100 Stat. 1213, reinforces the plain meaning of the statute. The predecessor provision to Section 1030(a)(5)(A) applied to anyone who "knowingly accesses a computer without authorization * * * and by means of such conduct knowingly * * * prevents authorized use of [] such computer." 18 U.S.C. 1030(a)(3) (Supp. II 1984). As the court of appeals correctly determined, Congress changed the *mens rea* requirement from "knowingly" to "intentionally" because it "sought only to proscribe intentional acts of unauthorized access, not 'mistaken, inadvertent, or careless' acts of unauthorized access." Pet. App. 9a, quoting S. Rep. No. 432, 99th Cong., 2d Sess. 5

[3] The same concerns animated the court's analysis in *United States* v. *Johnson & Towers, Inc.*, 741 F.2d 662 (1984), cert. denied, 469 U.S. 1208 (1985), where the Third Circuit held that a statute that proscribed knowingly "treat[ing], stor[ing], or dispos[ing] of any hazardous waste" requires proof that the defendant knew that the substance he stored was a hazardous waste. 741 F.2d at 667-669. Also of no help to petitioner are *Morissette* v. *United States*, 342 U.S. 246 (1952), and *United States* v. *United States Gypsum Co.*, 438 U.S. 422 (1978). In both of those cases, the Court construed a statute not to create a strict liability offense, in light of the historical tradition of requiring some *mens rea* for any criminal prohibition.

(1986); see H.R. Rep. No. 612, 99th Cong., 2d Sess. 5-6 (1986) (intent standard "meant to focus Federal criminal prosecutions * * * on those who evince a clear intent to enter, without authorization, computer files belonging to another"). In other words, the evil that Congress sought to combat was the intentional unauthorized accessing of computers.[4]

The change from the predecessor statute also demonstrates that Congress intended the *mens rea* requirement to apply only to the access portion of the statute and not to its damage conditions. The 1984 version of the statute applied the "knowingly" requirement to both its access and damage portions. Congress later rejected several similarly structured bills in favor of the bill it ultimately passed, which contains only one intent provision.[5] As this Court has stated, "Congress does not intend *sub silentio* to enact statutory language that it has earlier discarded in favor of other language." *INS* v. *Cardoza-Fonseca*, 480 U.S. 421, 442-443 (1987). In the case of computer fraud, Congress knew how to require a par-

---

[4] The House Report explained that the bill was targeted at computer "hackers," who were seen as "thrill seekers * * * trespassers, just as much as if they broke a window and crawled into a home while the occupants were away." H.R. Rep. No. 612, *supra*, at 5-6; *see* S. Rep. No. 432, *supra*, at 3.

[5] See S. 440, 99th Cong., 2d Sess. (1985) ("knowingly * * * access[] a computer * * * without authorization, * * * and thereby knowingly * * * cause[] or attempt[] to cause the withholding or denial of the use of such computer."); S. 610, 99th Cong., 1st Sess. (1985) ("knowingly accesse[d] without authorization a computer * * * and by means of such conduct affecting such operation, knowingly * * * modifie[d], destroy[ed], or prevent[ed], the use of information in such computer."); cf. S. 1678, 99th Cong., 1st Sess. (1985) (punishing one who knowingly and willfully without authorization damages a computer); H.R. 3381, 99th Cong., 1st Sess. (1985) (same).

ticular mental state for each aspect of the violation if it desired one.[6] In the statute that Congress enacted, however, it included an intent requirement only with respect to the unauthorized access of a computer.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

KENNETH W. STARR
Solicitor General

ROBERT S. MUELLER, III
Assistant Attorney General

MARK D. RASCH
ELLEN R. MELTZER
Attorneys

AUGUST 1991

---

[6] Although petitioner points to what the court of appeals called some "isolated language in the legislative history" (Pet. App. 13a) where congressional floor debates and reports expressed concern about "malicious damage" to computers, and "intentional damage" to computerized files, see Pet. 9-10, nothing in those brief passages suggests that the statute is limited to cases involving the intentional infliction of damage. Given Congress's rejection of the predecessor statute and other bills, petitioner's snippets of legislative history are not sufficient to show that Congress wanted an intent requirement to apply to each element of the offense.

Petitioner's contention (Pet. 11) that the difference between the 1986 statute and its 1984 predecessor is explained by drafting convenience is speculative at best. A comparison of the two statutes shows that the word "knowingly" was omitted from the damage provision in the 1986 version. While petitioner's explanation for the word's removal is plausible, the more natural explanation is that Congress did not want to attach a *mens rea* requirement to the damage provisions in the 1986 statute.

☆ U. S. GOVERNMENT PRINTING OFFICE: 1991 282081 45001